

Bradley P. Boyer (CA Bar No. 179430)
bradley.boyer@kutakrock.com
Saundra K. Wootton (CA Bar No. 224674)
saundra.wootton@kutakrock.com
KUTAK ROCK LLP
777 South Figueroa Street, Suite 4550
Los Angeles, CA 90017-5800
Telephone: (213) 312-4000

K. Jon Breyer* (MN Bar #302259)
(*Pro Hac Vice Application Forthcoming)
jon.breyer@kutakrock.com
KUTAK ROCK LLP
60 South Sixth Street, Suite 3400
Minneapolis, MN 55402
Telephone: 612-334-5000

Attorneys for Plaintiff,
MICHAEL MATTHEWS

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA – SAN JOSE DIVISION

MICHAEL MATTHEW,
Plaintiff,
v.
APPLE, INC., a California corporation
Defendant.

Case No.:

COMPLAINT FOR:

- (1) **INVASION OF PRIVACY**
- (2) **CONVERSION**
- (3) **TRESPASS TO CHATTELS UNDER CALIFORNIA LAW**
- (4) **CIVIL THEFT**
- (5) **UNJUST ENRICHMENT**
- (6) **INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS**
- (7) **NEGLIGENT INFLICTION OF EMOTIONAL DISTRESS**
- (8) **CIVIL CONSPIRACY**
- (9) **VIOLATION OF BUSINESS AND PROFESSIONAL CODE § 17200**

JURY TRIAL DEMANDED

Plaintiff Michael Mathews (“Mathews” or “Plaintiff”) hereby brings this Complaint against Apple Inc. (“Apple” or “Defendant”). Plaintiff states and alleges as follows:

///

NATURE OF THE ACTION

1
2 1. This action seeks the return of 2 TB of Plaintiff Mathews' data that Apple is holding
3 hostage in the iCloud, along with access to his Apple Accounts. The data consists of 30 years-worth
4 of private and personal data, including Social Security numbers, passport data, credit cards, bank
5 accounts, brokerage accounts and every website userID and password saved in the iCloud Key
6 Chain, as well as valuable work files, research, tax returns, photos, music, etc. In essence, Mathews'
7 entire digital life, including that of his family.

8 2. Mathews has been denied access to his data and accounts because Apple has
9 conspired with Hackers to deprive Mathews of his data. Apple has allowed the Hackers to exploit
10 a known flaw in Apple's data security that allows Hackers to gain access to victim's accounts and
11 set or alter the "Recovery Key." The Recovery Key is a 28-character code imbedded in an Apple
12 device, that once changed, provides the Hacker with sole control of the victim's accounts and
13 prevents the victim from remotely accessing the iCloud and accessing any files located in iCloud.

14 3. Once the Hackers change the Recovery Key, the owner of the Apple ID is locked
15 out of their accounts. With unmitigated access to the Apple ID password, thieves can steal money
16 via Apple Pay and other banking apps, view sensitive information like photos and emails, and more.

17 4. Apple's policy gives the owner of the Apple ID virtually no way back into their
18 accounts without the "Recovery Key" that is known only to the Hackers and Apple, but unknown
19 to the victim.

20 5. Even though Mathews is able to provide substantial and unquestionable evidence
21 that the accounts and the data in his Apple accounts are his, Apple nevertheless refuses to reset the
22 Recovery Key or allow Mathews access to his accounts and data. In so doing, Apple perpetuates
23 and aids the Hackers in their criminal activity.

24 6. This is an action for:

- 25 (a) Invasion of Privacy
26 (b) Conversion
27 (c) Trespass to Chattels
28 (d) Civil Theft

- (e) Unjust Enrichment
- (f) Intentional Infliction of Emotional Distress
- (g) Negligent Infliction of Emotional Distress
- (h) Civil Conspiracy
- (i) Violation of cal. Civ. Code § 17200

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §1332.

8. This Court has personal jurisdiction over Defendant Apple because it is authorized to and regularly conducts business in California and its principal place of business is in California.

9. Venue is proper under 28 U.S.C. §1391(b)(2) because, among other things, Defendant Apple's principal offices and business reside in this District, and therefore, are deemed to reside here for purposes of venue. Moreover, a substantial part of the events giving rise to this action occurred in this District and Plaintiff is being injured in this District.

INTRADISTRICT ASSIGNMENT

10. Pursuant to Civil Local Rule 3-2(c-e), a substantial part of the events giving rise of the claims herein arose in Santa Clara County and this action should be assigned to the San Jose Division.

PARTIES

11. Plaintiff Michael Mathews is an adult citizen and resident of Minnesota, residing in Maple Grove, Minnesota. Mathews maintained numerous Apple accounts under an Apple ID associated with the email Michael@MathewsXXXXXX.com¹ (the "Apple Accounts").

12. Defendant Apple is a California corporation with its headquarters and principal place of business at One Apple Park Way, Cupertino, CA 95014 which lies within this District. Apple is a resident and citizen of California. In addition to being headquartered and having its principal place of business in Cupertino, California, Apple transacts substantial business throughout the State of California, through advertising, marketing, and ownership of numerous Apple retail stores throughout California, including several in this District. Further, a substantial

¹ Plaintiff's email address has been redacted from the pleading but it has been disclosed to Apple.

part of the misconduct alleged in this Complaint occurred in and/or emanated from this district in California.

FACTUAL BACKGROUND

Apple's Recovery Key Provides Hackers a Means to Steal User Accounts

13. Apple designs, manufactures, markets and sells consumer devices including smartwatches, iPhones, iPads, Macbooks, and iMacs (collectively, "Apple devices"). Apple also provides services including but not limited to, the App Store, Apple Music, iMessage, iTunes, iCloud, FaceTime and more (collectively, "Apple Services" or "Apple accounts") that require logging in using an AppleID.

14. When a consumer purchases an Apple device or Apple Services, the purchased Apple device, and the data the consumer generates through the Apple Services, becomes the personal property of the consumer. Apple no longer has any ownership or property rights to the Apple devices or the data the consumer saves to iCloud.

15. Each Apple device and Apple account is associated with an AppleID that is the consumer (owner) email address, which is protected by an AppleID password.

16. With knowledge of an Apple device passcode, a hacker can easily reset the victim's AppleID password in the Settings app, even if Face ID or Touch ID is enabled. Subsequently, the hacker can turn off Find My iPhone on the device, preventing the owner of the device from tracking its location or remotely erasing the device via iCloud.

17. Using the stolen device to set or reset a Recovery Key, a randomly generated 28-character code that is required to regain access to an AppleID, a hacker can effectively lock a person out of their Apple accounts and use the information stored in the victim's Apple accounts to steal from the victim, open fictitious accounts in their name, and block the victim from gaining access to the accounts.

18. The Recovery Key is an extremely powerful tool that hackers have exploited. Apple has been aware of this security flaw for some time but has done nothing to correct it and, to make matters worse, has refused to allow victims to regain access to their accounts despite the flaw.

///

1 19. The Recovery Key was supposed to add a layer of protection, instead it has provided
2 hackers a way to circumvent the protections afforded Apple users. Even if a user has the Recovery
3 Key set to their desired 28-character code, a hacker need only obtain access to the Apple device
4 using the pin to gain access and create a Recovery Key or replace an existing Recovery Key directly
5 on the device.

6 20. Apple purportedly designed this feature in this way to allow users to reset their
7 forgotten Recovery Key. Instead, Apple has provided a very simple and effective way for hackers
8 to steal victim Apple accounts.

9 **Plaintiff Mathews Becomes a Victim**

10 21. On December 23, 2023, Plaintiff Mathews was pick-pocketed in Scottsdale,
11 Arizona. The thieves took Mathews' iPhone. Immediately upon learning that the iPhone had been
12 taken, Mathews contacted the Scottsdale police to file a report. It was too late. Within minutes of
13 the theft, the Hackers hacked into the iPhone, reset the Recovery Key, and took control of Mathews'
14 AppleID and iCloud accounts.

15 22. As a result, the Hackers have access to all of Mathews' Apple Accounts and his
16 private and personal data, more than 30 years-worth of material, including Social Security numbers,
17 passport data, credit cards, bank accounts, brokerage accounts and every website userID and
18 password that Mathews had saved in the iCloud Key Chain, including work files, research, tax
19 returns, photos, music, etc.

20 23. In addition to the devastating effect this has had on Mathews' personal data, the
21 iCloud also contains 30 years-worth of work-product that is the foundation for Mathews' business.
22 Mathews has 30 years of experience as a leading technology practitioner and executive, he has
23 collected, created and curated extensive research, presentations, content, experiences and the like
24 to develop his business. With the loss of his AppleID and all his iCloud content, his entire 30-year
25 document and knowledge base, and all the related tools, development efforts and products related
26 to his company are essentially "gone".

27 ///

28 ///

Apple Knowingly Aids the Hackers by Refusing to Allow Victims Access to Their Data

24. Apple's self-imposed policy of denying user access to their accounts without the Recovery Key is inherent unworkable, unfair, highly prejudicial, and extremely damaging. Although Mathews is able to provide (and did provide) Apple with all of the information needed to verify his identity and to ensure that the data he seeks access to is his, Apple flatly refuses to provide Mathews with access to his accounts and data. Instead, by its policy, Apple holds the Hacker in an elevated status, superior to that of the actual owner of the account, and provides the Hacker the unfettered access and ability to continue to steal user data, funds, accounts and to create false and fraudulent accounts using Plaintiff's identity.

25. This policy, and the willful and malicious acts of misappropriation and aiding in the Hackers stealing of Plaintiff's data and Apple Accounts, have been ratified, authorized and approved by an officer, director, or managing agent of Apple, who by virtue of their adoption of the policy, and the acts that support it, has committed an act of oppression, fraud, or malice.

26. With unmitigated access to a stolen iPhone, the device's passcode, and the Recovery Key, thieves can steal money via Apple Pay and other banking apps, view sensitive information like photos and emails, and harvest data from the iCloud that can be used to create fraudulent new accounts in the name of the user and essentially hijack one's entire digital life.

27. Apple's policy and design of its security features has long been known to Apple to be flawed, but they do nothing to fix it.

28. By its own self-created and inept limitations Apple gives users virtually no way back into their accounts without the Recovery Key – a Recovery Key that Apple knows the user cannot obtain.

29. The solutions to this colossal problem are easy, but Apple refuses to employ them:

- a. Change the policy so that the Recovery Key is not the only method to regain access to the account.
- b. Require the user's Face ID or Touch ID to make changes to the account, thus adding an hour-long delay before any actions can be performed. This additional layer of security aims to ensure that unauthorized individuals

cannot gain immediate access to the account and alerts the user of attempted unauthorized access.

c. Restrict how easy it is to delete the Recovery Key and create a new one.

d. Provide another way for users to confirm their identity, such as a social security number, passport, government ID or other reliable documentation.

30. Apple has made a policy decision to assist and perpetuate the lawlessness of criminals over the ownership and privacy rights of its users. Apple's actions are inexplicable and unconscionable and cannot stand. Apple must immediately provide Mathews access to and sole dominion over his accounts.

COUNT I

Invasion of Privacy

31. Plaintiff re-alleges the foregoing paragraphs as though fully restated herein.

32. Plaintiff has a legally protective privacy interest in his data and his Apple Accounts and a reasonable expectation of privacy with regard to his data and Apple Accounts.

33. Defendant willfully misappropriated Plaintiff's personal and private information, constituting a serious invasion of Plaintiff's privacy.

34. As a direct and proximate result of Defendant's misappropriation of Plaintiff's accounts, Plaintiff has lost the exclusive right of control over his personal information.

35. Defendant's actions have caused Plaintiff to experience and suffer anxiety, frustration, grief, and general mental anguish, all of which, in reasonable probability, will subsist in the future.

36. The intrusion is so serious as to constitute an egregious breach of the social norms, such that the misappropriation of Plaintiff's personal and private information is highly offensive.

37. Defendant acted with oppression and malice towards Plaintiff.

38. As Defendant intentionally and maliciously violated Plaintiff's right of privacy through misappropriating Plaintiff's data without the necessary consent, Plaintiff seeks compensatory damages to be determined at trial, and exemplary damages in a sum within the jurisdictional limits of this Court.

COUNT II

Conversion

39. Plaintiff re-alleges the foregoing paragraphs as though fully restated herein.

40. By preventing Plaintiff access to his data, Defendant has wrongfully exercised dominion and control over Plaintiff's property, *i.e.* money, bank accounts, Apps, services, music, books and/or content in Plaintiff's Apple Accounts (collectively, "Plaintiff's Data").

41. By unlawfully terminating Plaintiff's access to his data, and preventing him from regaining control of his accounts, Defendant has wrongfully exercised dominion and control over Plaintiff's Data.

42. Plaintiff has an ownership interest in, or has a right to the possession of Plaintiff's Data, and that which are only accessible using Plaintiff's Apple ID, which Defendant unlawfully, as set forth above, is maliciously withholding from Plaintiff.

43. Defendant intentionally interfered with the rights of Plaintiff when it unlawfully seized his Apple accounts and prevented him from accessing Plaintiff's Data.

44. Plaintiff did not consent to Defendant misappropriating Plaintiff's personal and private information.

45. Plaintiff demands the return of and access to Plaintiff's Data and his Apple Accounts.

46. This interference with Plaintiff's Data and Apple Accounts damaged Plaintiff in that he owns this data and can no longer access or utilize it.

47. Plaintiff is entitled to the return of Plaintiff's Data or the monetary value of the same.

48. Plaintiff seeks compensatory damages to be determined at trial and exemplary damages in a sum within the jurisdictional limits of this Court.

COUNT III

Trespass to Chattels

49. Plaintiff re-alleges the foregoing paragraphs as though fully restated herein.

50. Plaintiff at all relevant times has been the owner of the data in his Apple Accounts.

///

51. Defendant intentionally interfered and/or impaired Plaintiff's use of his Apple Accounts by permitting the Hackers to steal Plaintiff's accounts and data, and then prevented Plaintiff from being able to access Plaintiff's Data.

52. Plaintiff does not consent to Defendant's interference with and impairment to his access to his Apple Accounts and Plaintiff's Data.

53. Defendant's acts were the actual and proximate cause of injury to Plaintiff because it actually and substantially harmed Plaintiff by preventing Plaintiff from accessing Plaintiff's Data and his Apple Accounts.

54. Defendant's interference and impairment was malicious and oppressive.

55. Defendant knew and intended that their conduct would cause injury to Plaintiff.

56. Defendant acted despicably and with conscious disregard of Plaintiff's rights.

57. As a result of Defendant's interference with and impairment of Plaintiff's rights, Plaintiff is entitled to recover the actual damages he has suffered in an amount to be determined at trial, as well as punitive damages in an amount to be determined at trial.

COUNT IV

Civil Theft

58. Plaintiff re-alleges the foregoing paragraphs as though fully restated herein.

59. Pursuant to California Penal Section 496(c), a person who receives any property that has been stolen or that has been obtained in any manner constituting theft or extortion, knowing the property to be so stolen or obtained, or who conceals, sells, withholds, or aids in concealing, selling, or withholding any property from the owner, knowing the property to be so stolen or obtained, shall be liable for civil theft, which is punishable by treble damages, costs of suit, and reasonable attorney fees.

60. Defendant has stolen and withheld Plaintiff's property and has withheld and aided in the withholding of Plaintiff's property knowing the property (Apple Accounts and Plaintiff's Data) has been stolen or unlawfully obtained.

///

///

61. As a result of Defendant's civil theft, Plaintiff is entitled to recover the actual damages he suffered in an amount to be determined at trial, as well as treble damages in an amount to be determined at trial.

COUNT V

Unjust Enrichment

62. Plaintiff re-alleges the foregoing paragraphs as though fully restated herein.

63. By its wrongful, illegal, and unconscionable acts and omissions described herein, Defendant is unjustly enriched at the expense of Plaintiff.

64. Plaintiff conferred a benefit on Defendant when he purchased an Apple device and/or created an Apple ID, purchased content and uploaded data to the iCloud. By its wrongful, illegal, and unconscionable acts and omissions described herein, including preventing Plaintiff from accessing his Apple Accounts and Plaintiff's Data, Defendant has been unjustly enriched at the expense of Plaintiff.

65. Plaintiff's detriment and Defendant's enrichment were related to and flowed from the wrongful, illegal, and unconscionable conduct detailed in this Complaint.

66. Defendant has profited from their unlawful, unfair, unconscionable, and illegal practices at the expense of Plaintiff under circumstances in which it would be unjust for Defendant to be permitted to retain the benefit. It would be inequitable for Defendant to retain the profits, benefits, and other compensation obtained from its wrongful, illegal, and unconscionable conduct as described herein.

67. Defendant has been unjustly enriched in retaining the revenues derived from Plaintiff's purchases of an Apple device and/or creation of an Apple ID and/or purchases of content, which retention of such revenues under these circumstances is unjust and inequitable because Defendant prevents Plaintiff from accessing any of his Apple Accounts and Plaintiff's Data, which caused injuries to Plaintiff because he would not have created an Apple ID or Apple Accounts on the same terms had he been advised of Defendant's wrongful, illegal, and unconscionable conduct as described herein.

///

69. As a direct and proximate result of Defendant's wrongful conduct and unjust enrichment, Plaintiff is entitled to restitution of, disgorgement of, and/or imposition of a constructive trust upon all profits, benefits, and other compensation obtained by Defendant for its inequitable, unconscionable, and unlawful conduct.

Intentional Infliction of Emotional Distress

77. Defendant must pay damages in an amount to be determined at trial as compensatory damages for emotional pain, suffering, and mental anguish, and exemplary damages in a sum within the jurisdictional limits of this Court.

Negligent Infliction of Emotional Distress

79. Defendant's conduct toward Plaintiff was malicious, extreme, and outrageous and caused significant emotional harm and mental distress.

84. Defendant must pay damages in an amount to be determined at trial as compensatory damages for emotional pain, suffering, and mental anguish, and exemplary damages in a sum within the jurisdictional limits of this Court.

Civil Conspiracy

89. Apple and the Hackers conspired, coordinated, and/or engaged in other behavior and concerted action to accomplish the unlawful objective of depriving Plaintiff of his Apple Accounts, Plaintiff's Data, and rights due to him under the above-mentioned laws and to cause

1 harm to Plaintiff.

2 90. Such concerted action did cause harm to Plaintiff including but not limited to
3 emotional distress and loss of 30 years-worth of personal and professional data.

4 91. Defendant Apple was aware that Plaintiff's Data had been compromised through a
5 security design flaw and aided, assisted and conspired with the Hackers to lock Plaintiff out of his
6 account and provide the Hackers unfettered access to Plaintiff's Data.

7 92. Defendant Apple has acted with malice towards Plaintiff.

8 93. Because Defendant Apple is guilty of conspiring to harm Plaintiff, Defendant must
9 pay compensatory damages to Plaintiff and exemplary damages in a sum within the jurisdictional
10 limits of this Court.

11 **COUNT IX**

12 **Violation of California Business and Professional Code Sec. 17200**

13 94. Plaintiff re-alleges the foregoing paragraphs as though fully restated herein.

14 95. Defendant has engaged in unlawful, unfair, or fraudulent acts or practices, which
15 constitute unfair competition within the meaning of Section 17200 of the California Business and
16 Professions Code.

17 96. Specifically, Defendant:

- 18 (a) Violated California Civil Code section 1798.81.5, subdivision (b), which
19 requires Defendant to implement and maintain reasonable security
20 procedures and practices appropriate to the nature of the personal
21 information that Apple maintains, to protect the personal information from
22 unauthorized access, destruction, use, modification, or disclosure;
- 23 (b) Engaged in unfair acts or practices regarding Apple's data security practices
24 at the time of the breach; and
- 25 (c) Made unfair, deceptive, untrue, and misleading statements regarding Apple's
26 data security practices at the time of the breach.

27 ///

28 ///

97. Because of Defendant's acts, Defendant must pay restitution to Plaintiff as a result of Defendant's unlawful, unfair and/or fraudulent business practices, and return and grant exclusive access to Plaintiff his data and Apple Accounts.

WHEREFORE, Plaintiff requests that this Court grant the following relief:

1. An award of damages sustained by Plaintiff as a result of Defendant's conduct, including all direct, incidental and consequential damages in an amount greater than \$5,000,000, the exact amount to be determined at trial;
2. Punitive damages in a sum within the jurisdictional limits of this Court;
3. Treble damages pursuant to California Penal Section 496(c);
4. Restitution under California Business and Professions Code Section 17200;
5. Injunctive relief in the form of reestablishing Plaintiff's access to and exclusive dominion over Plaintiff's Data and Apple Accounts;
6. An award of attorneys' fees, costs and disbursements incurred in this action;
7. An award of prejudgment and post-judgment interest as allowed by law; and
8. An award of such other and further relief as the Court may deem just and equitable.

DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury in this case on all issues so triable.

Dated: January 16, 2024

KUTAK ROCK LLP

By: /s/ Bradley P. Boyer

Bradley P. Boyer
Saundra K. Wootton
K. Jon Breyer, (*Pro Hac Vice Application*
Forthcoming)
Attorneys for Plaintiff,
MICHAEL MATTHEWS

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28